Whereas Learning Analytics uses data to inform decisions – from individual to curriculum level – concerning students' learning, data may also be used to inform decisions about their wellbeing. Possible applications cover a very wide range: from screen-break reminders to alerts when a student appears to be at risk of suicide. Clearly this can involve both significant benefits and high risks.

Voluntary wellbeing apps – where each individual makes a positive choice to be monitored – could be provided on the basis of "consent", though this requires high standards of both the information given to users and the form of consent. If, however, an organisation wishes to proactively identify possible wellbeing problems across all students or staff, rather than waiting for individuals to self-report, then the most suitable bases under UK and EU data protection law appear to be provisions on "confidential counselling services"[1] or "preventive or occupational medicine".[2]

The approach taken by Jisc's Code of Practice for Learning Analytics provides a good basis for wellbeing applications: this Annex indicates – using that Code's headings – where wellbeing practice is likely to differ.

Responsibility

The law requires that processing for preventive medicine must be done "under the responsibility of a professional subject to the obligation of professional secrecy". For wellbeing applications, UUK suggests that such regulated professionals should be found in Student Support Directorates;[3] both Jisc and UUK recommend "extensive consultation with mental health and student counselling specialists".[4] Provided policies and processes remain "under the responsibility" of such professionals, day-to-day operations can be assigned to appropriately trained tutors and other staff in accordance with appropriate confidentiality rules.

Transparency and Consent

Legal requirements for these are likely to be stronger in health-related applications. Where consent is used as a basis for processing (e.g. for installing a wellbeing app, providing additional data, or informing a tutor of contact with a counselling service) there must be "explicit" agreement to the purpose(s) for which the data will be used. In the ICO's view this requires a separate "express statement of consent" for each purpose.[5] Thus, for example, a student who provides health information for their examination or lecture arrangements should have a separate choice whether or not that information is also used in wellbeing assessments. Particular care must be taken to inform individuals if unexpected data (e.g. finance) are incorporated into models, and to enable them to check and correct their own data.

---

[1] *Data Protection Act 2018* Schedule 1 Part 2 section 17
[2] *Data Protection Act 2018* Schedule 1 Part 1 section 2 and *General Data Protection Regulation* Article 9(2)(h)
[3] https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2018/guidance-for-sector-practitioners-on-preventing-student-suicides.PDF
[4] http://repository.jisc.ac.uk/6916/1/student-wellbeing-and-mental-health-the-opportunities-in-learning-analytics.pdf
[5] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what5

Privacy

As for Learning Analytics, systems must be designed to protect individuals' privacy. Health-related processing and data are likely to require tighter restrictions (both technical and organisational) than that relating to learning. Medical confidentiality standards should be the norm.

Validity

Given the high risks of adverse consequences (see below) it is essential to ensure that data and predictions derived from them are relevant and accurate. Processing to develop and test algorithms should be kept separate from processing leading to interventions with individuals to ensure that, for example, validation data does not leak into the intervention process and testers are not able to identify individuals.

Access

As for learning analytics, individuals have a right of access to their personal data. For data concerning health, however, organisations must first consult with the "relevant health professional" to ensure that disclosing the information is not likely to cause serious harm to the physical or mental health of the data subject or another individual.[6]

Enabling Positive Interventions/Minimising Adverse Impacts

As with Access, some interventions carry a risk of making a wellbeing problem worse, rather than better. Talking to someone about stress, depression or suicide requires both training and readily available support. Data and algorithms will flag individuals with widely differing needs: personalised support is likely to be needed.

Organisations should therefore consider which interventions should be provided in a medical context in case of a negative reaction, and should ensure that they can provide appropriate support before implementing any wellbeing application.

Stewardship

Wellbeing applications that aim to derive information about an individual's health are likely to represent a high risk to privacy, and thus require a formal Data Protection Impact Assessment (DPIA).[7] Where this risk cannot be mitigated, the law requires prior consultation with the national Data Protection Regulator – in the UK, the Information Commissioner's Office.

[6] *Data Protection Act 2018* Schedule 3 Part 2

[7] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/